

## Forum:[Hack Forums](#)

Thread: [UID 2676098 \(xBc\) selling backdoored scripts](#)

**Nob** - June 11, 2016, 3:37 pm

Hello,

So a fun one for you guys tonight.

This guy : [xBI?c?](#) is selling backdoored scripts on [this thread](#).

I actually bought his OVHX script to see what it was looking like.

First odd thing, my antivirus detected it, while it never rings the bell for any of the scripts I own. That was awkward. I said it was a false positive, and uploaded it to my "sandbox" server (a 5\$ DigitalOcean VPS where I test everything before putting into production). Before running it, I did a "strings" on the file, and, surprise, you'll never guess what I found !

The first thing the script does is this :

It loads a shortened link. This shortened link is hiding the URL to a IP-grabbing service (grabify.link), so it grabs the IP of your server when you load it.

It then goes into /etc/passwd and gives permission to a user that hasn't been created yet (it's coming). And it deletes all the log files with "rm -rf /var/log".

Then it does this :

It actually adds the user that was given permissions above into the Unix password manager.

It's then very easy for this guy to access your server, as he obtained the IP with grabify and added his own credentials into it.

As a broader advice, always strings scripts you found on the internet. You never know what's inside.

Regards

**Ooze** - June 11, 2016, 3:43 pm

You should crack the hash, and hack his shit

But anyway, I can't verify this is true but this is why Community Alerts exist

**Nob** - June 11, 2016, 3:47 pm

(Jun 11, 2016 03:43 PM)The JOker Wrote: [\[CITE\]](#) You should crack the hash, and hack his shit

But anyway, I can't verify this is true but this is why Community Alerts exist

I don't really specialize in hash cracking but I guess someone could here, here is the plain text for it :

Spoiler [\(Click to View\)](#)

'\$6\$TwPdKvSI\$6RkfcsCjpVw5CXpAqfVBEiPTa1s/iwoYBf7bogLY08/N8d3WKfgKKSKstlCtFXFrpUwQ9nJukjvKXyg7cmRev1:16840:0:99999:7:::

**IHitNoobs** - June 11, 2016, 3:47 pm

this looks interesting man good find man thanks for the heads up

**illuminati** - June 11, 2016, 7:20 pm

Kid is also a scammer. He revenge negged me so be careful. ?

**gochi** - June 11, 2016, 9:48 pm

This guy is a scammerr, scammed \$325.

Thread: <https://hackforums.net/showthread.php?tid=5297976>

Also revenge negged me for reporting his scam.

**PRPS** - June 11, 2016, 9:53 pm

Gonna have to start using sandbox. people are scary out here. lol

**Bl?c?OuT** - June 12, 2016, 1:26 am

I'm using this script every day..much stresser have it like finestmoddingstresser.net, this script isn't mine , i heve bought it and i use it every day.

**Agonises** - June 12, 2016, 1:28 am

(Jun 12, 2016 01:26 AM)xBl?c? Wrote: [\[CITE\]](#) I'm using this script every day..much stresser have it like finestmoddingstresser.net, this script isn't mine , i heve bought it and i use it every day.

No no no, of course you use the script every day.

**Nob** - June 12, 2016, 6:25 am

Well, if other stressers use it, it means you better tell them their servers are rooted ...

**JohnAnonDoe** - June 15, 2016, 9:05 am

Where is the script exactly? I only see him selling VPS and Dedi's.

Also, everyone be careful running scripts under sudo (root) (especially from untrusted sources)

**DarkN3ss61** - June 15, 2016, 12:45 pm

(Jun 14, 2016 02:32 PM)Stratos Wrote: [\[CITE\]](#) Seriously plain text...? Could have at least xor'd it. Should hit that link with a layer 7 flood using wget useragent.. then he can have fun finding out which IP were roots lmao.

Oi don't hit my ip logger with a 7 layer flood lmao

**Kyle1995** - June 15, 2016, 12:49 pm

This is so hilarious, I can't believe it